UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI

UNITED STATES OF AMERICA

V. CRIMINAL NO. 3:21-CR-107

JAMARR SMITH, et al.

GOVERNMENT'S RESPONSE TO DEFENDANTS' MOTION TO SUPPRESS

Comes now the United States of America, by and through the United States Attorney for the Northern District of Mississippi, and in response to defendants' Motion to Suppress would respectfully show unto the Court the following, to wit:

The search warrant at issue authorized disclosure from Google of approximately two hours of location information associated with electronic devices that were in close proximity to the Lake Cormorant Post Office at the time that Sylvester Cobbs, a contract carrier of the U.S. Postal Service, was robbed of U.S. Mail matter, money, and property at that location. The geofence warrant issued by Magistrate Judge Roy Percy complied with the Fourth Amendment as it was based on probable cause and specified its object with particularity. Alternatively, agents relied upon the warrant in good faith. Accordingly, the defendants' Motion to Suppress should be denied.

FACTS

On February 5, 2018, three individuals, acting in concert, robbed Sylvester Cobbs of U.S. Mail matter, money, and property at the Lake Cormorant Post Office in Lake Cormorant, Mississippi. The Lake Cormorant Post Office is open in the mornings, closing to the public at approximately noon. Sylvester Cobbs is a contract carrier for the U.S. Postal Service who would

run a route in the afternoons collecting mail from U.S. Post Offices in Tunica and DeSoto Counties to take to the distribution center in Memphis. The Lake Cormorant Post Office was the fourth of five stops he would make along his route.

The bags of mail collected by Cobbs along his route included the registered mail bags. In addition to registered mail, the registered mail bags contain the cash receipts collected by the Postal Service from the sale of items such as postal money orders, stamps, etc. By the time Cobbs stopped at Lake Cormorant, he had already collected the registered mail bags from three other post offices along his route.

On February 5, 2018, at approximately 5:20 p.m., Cobbs pulled into the parking lot of the Lake Cormorant Post Office in a large U.S. Mail truck and backed up to the back door, where he would use his key to retrieve the mail bags waiting for him inside the Post Office. Before he could open the back door to the Post Office, an unknown individual, later determined to be Gilbert McThunel, came out of his hiding place behind the Post Office intent on robbing Cobbs of the registered mail bags that Cobbs had collected at his previous stops. When Cobbs did not cooperate, McThunel struck Cobbs multiple times with a handgun, then grabbed the registered mail bags from Cobbs' truck. Cobbs pulled the truck to the front of the Post Office and called for help.

When the U.S. Postal Inspection Service began its investigation, agents determined that there was a security camera on a farmer's shop across the street.[1] The camera was aimed at the side of the Post Office where the aforementioned attack and robbery occurred. From a review of

1 The security camera footage is submitted as Exhibit "A" to the government's response. The timer on the security footage starts at 00:00, so that references to times on the security footage are not to the specific time of the robbery, but simply to a time frame on the footage itself.

the security footage, agents began to develop an understanding of the events of the robbery. Prior to the robbery, the video depicts a white SUV driving past the side of the Post Office opposite the attack. The SUV leaves the picture then returns into view a short time later, stopping briefly to let someone, later determined to be McThunel, out of the vehicle. The SUV drives off and McThunel walks to the back of the Post Office where he hides behind the building and waits for Cobbs to arrive. While waiting for Cobbs to appear, video footage shows McThunel with his left arm and hand held up to his ear for multiple minutes, consistent with talking on a phone. (Exhibit "A," 6:50 minute mark to 9:50 minute mark) Phone records later confirmed that McThunel was indeed on the phone. McThunel received a call at 5:16 p.m. from Jamarr Smith, another participant in the robbery, who was acting as a lookout, and the two engaged in a 5 minute, 42 second phone call.

When Cobbs arrives, video footage shows McThunel attacking Cobbs as described above, then grabbing the registered mail bags out of the back of Cobbs' truck. Part of the confrontation between McThunel and Cobbs is obscured by the truck, but it is clear from the video that McThunel struck Cobbs multiple times, driving him to the ground. As Cobbs pulls the truck to the front of the Post Office, McThunel is seen pacing back and forth behind the Post Office for a short period of time, before eventually exiting the camera's view walking away from the Post Office to the left of the camera (behind the Post Office). Before leaving the camera's view, McThunel sets the registered mail bags down and appears to reach briefly into his pocket. While it is difficult to see exactly what he is doing, it appears that McThunel is possibly pulling out a phone to check for a text message or to see who is calling. (Exhibit "A," 13:34 minute mark) McThunel walks out of view of the camera for several seconds, then returns to the back of the Post Office. McThunel

sets the registered mail bags on the ground and squats down, and while it is again difficult to see what he is doing as he is squatting, it appears that he may be checking or texting on his phone. (Exhibit "A," 13:58 minute mark to 14:07 minute mark) McThunel then stands up and walks out of view again. A short time later, the white SUV returns, approaching from the front of the Post Office and driving past the opposite side of the Post Office, in the direction that McThunel was last seen walking.

Agents also noticed another vehicle of interest that was caught on camera during the course of the robbery. Shortly after Cobbs pulled into the Post Office parking lot, a red Hyundai Sonata, following from the same direction as Cobbs' truck, approached the intersection in front of the Post Office, slowed to a brief, but noticeable and odd stop in the intersection, then completed a right hand turn, travelling across the railroad tracks where the car made a u-turn and came back the direction from which it had come. Approximately a minute and a half later, as the attack on Cobbs is occurring, the same car approaches the intersection in front of the Post Office, stops in the intersection again, before making a u-turn in the intersection and pulling in front of a building across the street from the front of the Post Office. The car stops for several seconds in front of the building, then backs up a few feet towards the Post Office, where it sits for several seconds until Cobbs gets in his truck and moves the truck to the front of the Post Office. As Cobbs pulls to the front of the Post Office, the car pulls forward and leaves the scene.

An eyewitness who lived in the area had seen the red Sonata sitting in the area near the Post Office at the time of the robbery and had approached the driver to ask the driver if he needed any assistance. This witness later identified the driver of the red Sonata as Jamarr Smith (after

agents had developed Smith, McThunel, and Thomas Iroko Ayodele as subjects of the investigation).

Agents were unable to identify any suspects from the video footage, so in November of 2018, Todd Matney of the U.S. Postal Inspection Service prepared an affidavit seeking a geofence search warrant, with assistance from another Postal Inspector, Stephen Mathews. The geofence warrant, directed to Google, sought information pertaining to any Google accounts located within a described geographical box between 5:00 pm and 6:00 pm, central time, on February 5, 2018. The geographical box, drawn with specific latitude and longitude coordinates, essentially encompassed the Lake Cormorant Post Office and a portion of the road to the front and the side of the Post Office where the vehicles of interest were seen travelling. The warrant set forth a specific three-step process for obtaining information from Google. Google would first provide agents with a list of Google accounts found within the "box" during the specified time frame, with the devices only identified by an anonymous numerical identifier, without any content concerning the user of the device. (Step One). For those accounts that the agents determined to be relevant to the investigation, Google would provide additional location history outside of the "box" to determine path of travel. (Step Two). This additional location information would not exceed 60 minutes either side of the first and last timestamp associated with the account in the initial dataset. Finally, for those accounts deemed relevant following Step Two, Google would provide subscriber information to the agents. (Step Three).

The affidavit and application for a search warrant were submitted to Magistrate Judge Roy Percy for review. On November 8, 2018, Judge Percy issued the geofence warrant. The agents followed the steps set forth in the warrant. In response to the first step, Google provided

information showing that three devices had been located within the "box" during the specified time. Two of the devices, identifiers ending in 859 and 768, registered multiple times between 5:22 and 5:30. One of the devices, identifier ending in 479, only registered once, at 5:58. Agents determined that devices 859 and 768 were relevant and that device 479 was not. Agents followed the process set forth in the warrant for steps two and three, eventually finding out that devices 859 and 768 belonged to Smith and McThunel. Further investigation, including phone records pertaining to Smith and McThunel, revealed Thomas Iroko Ayodele as a potential subject. Agents determined that Ayodele owned a white SUV that appeared to match the SUV caught on camera at the scene of the robbery. Agents further determined that McThunel owned a red Hyundai Sonata that appeared to match the red Sonata caught on camera and in which Smith was identified by an eyewitness as driving in the vicinity of the Post Office at the time of the robbery. Other location information obtained through search warrants issued to phone companies showed the three defendants travelling from Batesville (their hometown) to Lake Cormorant and back on the afternoon of the robbery and phone records further confirmed multiple communications between the defendants throughout the time immediately before, during, and after the time of the robbery.

LEGAL ANALYSIS

Geofence warrants in general are a valid investigatory tool of law enforcement and this warrant in particular was a lawful warrant supported by probable cause. Furthermore, even if the court were to determine that the magistrate judge erred in issuing the warrant, the good faith exception would apply so that defendants' Motion to Suppress should be denied.

A. The Geofence Warrant Satisfied the Fourth Amendment

The geofence warrant at issue here authorized the government to obtain from Google

limited and specified information directly tied to a particular robbery at a particular place and time.[2] The facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is not a general warrant. When law enforcement officers sought the warrant, they were investigating a serious violent crime, wherein the victim, Sylvester Cobbs, had been beaten with a handgun. The geofence warrant allowed them to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only a fair probability that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause is not a high bar. *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). The duty of a reviewing court is simply to ensure that the magistrate judge had a substantial basis for concluding that probable cause existed. *Gates*, 462 U.S. at 238–39.

Here, the affidavit in support of the warrant established an ample basis for the issuing magistrate judge's finding of probable cause. The affidavit established that an unknown subject, aided and abetted by two other unknown subjects, robbed Sylvester Cobbs of matter, money, and property belonging to the U.S. Postal Service. *See* Affidavit paragraphs 10-15. It further established that the unknown subject was "possibly using a cellular device both before and after the robbery." *See* Affidavit paragraph 16. The affidavit established that this was a premeditated

2 The defendants make reference in their memorandum to general warrants, but the warrant at issue here did not remotely resemble a general warrant. A general warrant "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, as discussed herein, the warrant at issue here was limited to specified information directly tied to a particular robbery at a particular place and time.

crime involving multiple offenders and that the subjects likely used cell phones to communicate during the robbery. *See* Affidavit paragraph 18. It established a connection between smartphones and Google location information. *See* Affidavit paragraphs 6-9. It explained that nearly every Android phone has an associated Google account, and that Google collects and retains location data from such devices when the account owner enables Google location services. *See* Affidavit paragraphs 8. It also explained that Google can collect location information from non-Android smartphones if the devices are registered to a Google account and the user has location services enabled. *See* Affidavit paragraphs 8. From this information, there was a substantial basis for the magistrate judge to find probable cause to believe that Google possessed evidence related to the robbery.

In the Matter of the Search of Information that is Stored at the Premises Controlled by Google LLC., 579 F. Supp. 3d 62 (D.D.C. 2021) (hereinafter referred to as *Google V*[3]) provides a particularly instructive opinion on geofence warrants. In that case, the magistrate judge issued a memorandum opinion explaining, in great detail, his reasoning for issuing a geofence warrant. The opinion contains a good summary of the technological aspects behind a geofence warrant, as well as a strong legal analysis of issues such as probable cause and particularity.

As set forth in the magistrate judge's opinion, probable cause is a "practical, nontechnical conception" drawn from "common-sense conclusions about human behavior." *Google V*, 579 F. Supp. 3d at 74 (citing *Illinois v. Gates*, 462 U.S. 213, 231 (1983)). It "deals with probabilities and depends on the totality of the circumstances," *Id*. at 75 (citing *Maryland v. Pringle*, 540 U.S.

3 This opinion will be designated as *Google V*, so as not to be confused with other opinions cited therein listed as *Google I-IV*.

366, 371 (2003)), and is "a fluid concept ... not readily, or even usefully, reduced to a neat set of legal rules." *Id*. (citing *Gates*, 462 U.S. at 232). Thus, the test for probable cause is not reducible to "precise definition or quantification." *Id*. (citing *Pringle*, 540 U.S. at 371).

The magistrate judge went on to explain that for search warrants, probable cause requires (i) a "fair probability" that a crime has been committed and (ii) "a fair probability that contraband or evidence of [that] crime will be found in a particular place." *Google V*, 579 F. Supp. 3d at 75 (citing *Gates*, 462 U.S. at 238). In other words, the core inquiry is whether the warrant application provides "a 'substantial basis' for concluding that 'a search would uncover evidence of wrongdoing'" by "demonstrat[ing] cause to believe that 'evidence is likely to be found at the place to be searched'" and "'a nexus ... between the item to be seized and criminal behavior.'" *Id*. (citing *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017)).

In analyzing the issue of probable cause, the magistrate judge in *Google V* found that there was a fair probability that the search of Google's servers would uncover useful evidence pertaining to the identities of the suspects:

> First, there is more than a "fair probability" that the suspects were within the geofence during the time windows the government established. The requested geofence encompasses the [Redacted] center and its parking lot. The CCTV footage obtained by the government shows the suspects inside the [Redacted] center.
>
> Second, the government has evidence that the suspects were actually using cell phones during the time windows set in the warrant. The CCTV footage apparently shows the suspects utilizing their devices while inside the [Redacted] center.
>
> Third, the affidavit's failure to specifically allege that the suspects, while on their phones, were using applications or other features that would communicate location data to Google, is also not fatal to the warrant application. The probability that the phones were communicating location information to Google is, at the very least, "fair," and that is all that is required.
>
> Fourth, there is also a "fair probability" that Google is in possession of identifying

information for the users of phones found within the geofence.

Google V, 579 F. Supp. 3d at 77-79. Accordingly, the magistrate judge determined that probable cause existed for the issuance of the warrant. Of particular interest was the magistrate judge's determination that the government need not show that any of the suspects were actually using their phones within the parameters of the geofence. As stated by the court:

> In the Court's view, however, it is not necessary that the government actually know that suspects are using their phones within the geofence. *See Google III*, 497 F. Supp. 3d at 355 (granting geofence warrant despite there being "no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense"). The core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business. *See id*. at 356 ("Unlike virtually any other item, it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person."); *see also United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021) ("Even if nobody knew for sure whether the [suspect] actually possessed a cell phone, the judges were not required to check their common sense at the door and ignore the fact that most people 'compulsively carry cell phones with them all the time.'" (quoting *Carpenter*, 138 S. Ct. at 2218)).

Google V, 579 F. Supp. 3d at 78.

Similar to the facts of *Google V*, there was more than a fair probability that the suspects were within the geofence during the time period referenced in the warrant, as shown on the video footage from the security camera across the street. While not even necessary, the government had evidence that the suspects were using cell phones during the time in question. This belief later proved to be corroborated by the defendants' phone records. The probability that the suspects cell phones were communicating location information to Google was at least fair. There was also a fair probability that Google was in possession of identifying information for the users of the phones found in the geofence. Accordingly, probable cause was satisfied.

Another case that is instructive on the issue of probable cause is *United States v. James*,

2019 WL 325231 (D. Minn. 2019), wherein the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* Here, where McThunel used his phone just before the robbery, the basis for the magistrate judge's finding of probable cause was even stronger than that in *James*.

Messerschmidt v. Millender, 565 U.S. 535 (2012), demonstrates that the Supreme Court does not narrowly construe what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

Similarly, the issuing magistrate judge here had multiple reasons to believe that the location information for those present at the robbery would constitute evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of

the crime. They could use it to identify the robber and any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the assailant, including an attempt by the assailant to blame someone else for his crime. Thus, probable cause existed because the information sought by the warrant was in fact evidence appropriately seized pursuant to a search warrant. The issuing magistrate judge had a substantial basis for finding probable cause to believe that Google possessed location information regarding the scene of the robbery, and this Court should therefore deny the defendants' motion to suppress.

Finally, the defendants argue that the geofence warrant collected information about persons not suspected of criminal activity, but this fact does not aid their Fourth Amendment argument. The Supreme Court has held that "it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime." *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). Instead, a search warrant "may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id.* Furthermore, the Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). The defendants therefore lack standing to challenge the government's acquisition of others' location information. *See, e.g., United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Additionally, these other individuals, like the defendants (as will be discussed below),

voluntarily disclosed their location information to Google. Google's disclosure of their location information therefore did not infringe their Fourth Amendment rights.

The defendants rely upon *Ybarra v. Illinois* to support their assertion that the warrant was overbroad, but *Ybarra* is not applicable. *Ybarra* addressed a physical search of a person, rather than simply obtaining information about a person, as we have in the present matter. *Ybarra*, 444 U.S. 85, 91 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.")

2. The Geofence Warrant Specified its Objects with Particularity

Under the Fourth Amendment, a valid warrant must particularly describe the place to be searched, and the persons or things to be seized. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The particularity requirement constrains a warrant so that it is no broader than the probable cause on which it is based. *Williams v. Kunze*, 806 F.2d 594, 598-599 (5th Cir. 1986). It protects against exploratory rummaging in a person's belongings by requiring a particular description of the things to be seized. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). Moreover, the test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Further caselaw pertaining to the issue of particularity is set forth in detail in *Google V*. As stated by the magistrate judge, the manifest purpose of the particularity requirement was to prevent general searches. *Google V*, 579 F. Supp. 3d at 75 (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). Therefore, "[s]earch warrants must be specific." *Id*. (citing *United States v. Manafort*, 313 F. Supp. 3d 213, 231 (D.D.C. 2018)). There are two prongs of specificity:

particularity and breadth. *Id*. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id*. at 75-76 (*citing Manafort,* 313 F. Supp. 3d at 231). A warrant is not constitutionally overbroad so long as the time, location, and overall scope of the search are consistent with the probable cause set forth in the warrant application. *Id*. at 76.

In regard to time, the court in *Google V* stated:

> [T]he geofence only provides cell phone users' whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements. Thus, viewed in proper context, the government's request is limited and reasonable.

Google V, 579 F. Supp. 3d at 81. As to location, the magistrate found "[T]he inquiry here is whether the 'target locations [are] drawn to capture location data from locations at or closely associated with the [crime].'" *Id*. at 82 (citing *Google III*, 497 F. Supp. 3d at 358).

In addressing whether or not the requested warrant was overbroad, the court in *Google V* stated:

> The geofence may also capture the location information for persons who are not suspects, namely the other customers inside the [Redacted] center….For several reasons, the warrant's potential to collect location information from these other individuals does not render it deficient….As an initial matter, constitutionally permissible searches may infringe on the privacy interests of third persons—that is, persons who are not suspected of engaging in criminal activity. The Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches….The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—that the privacy interests of third parties uninvolved in criminal activity would be implicated….Rather, the Fourth Amendment seeks to ensure that privacy interests are not infringed by law enforcement activities without a showing of probable cause and a particularized description of the place to be searched and the things to be seized.

Google V, 579 F. Supp. 3d at 82-84.

Here, the geofence warrant was narrowly constrained based on location, date, and time. The warrant sought only location and identity information from Google regarding a one-hour interval for individuals present at the site of a robbery. Based on the facts and circumstances agents knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the assailant and his co-conspirators.

The cell tower dump opinion *United States v. James* provides further persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants were sufficiently particular because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the geofence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The parameters of the geographical box set forth in the geofence warrant is smaller than most cellular sites, and the government only obtained location information regarding three individuals,[4] rather than hundreds or thousands.

The defendants argue that the warrant lacked particularity, stating that the warrant left too much discretion to Google and the government to negotiate which users would have their account

4 One of which was never identified, as the information obtained indicated that individual was not relevant to the investigation.

information searched. In actuality, the warrant specifically stated that it sought files and records maintained by Google Inc., believed to conceal location information, subscriber information, and other evidence as set forth in the affidavit. There were very limiting constraints as to time and place for which the government was seeking location information. In an effort to further limit the information obtained by the government, a three-step process was set forth to assist the government in narrowing the subscriber information provided by Google to only those accounts that appeared to be relevant to the investigation, information that would be less than the maximum quantity of location and identity information that the warrant authorized. The warrant, however, established probable cause for all the evidence that law enforcement could have obtained: identity information and two-hours of location data for all individuals present at the site of the robbery during the time of the robbery. The information specified by a warrant must be no broader than the probable cause on which it is based, *Kunze*, 806 F.2d at 598-599, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

The assertion that the warrant lacked particularity is simply without merit.

B. Evidence from the Geofence Warrant Should Not Be Suppressed Because Investigators Relied upon it in Good Faith

Even assuming the geofence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search

or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there are few judicial opinions (perhaps none in November 2018 when the warrant was sought[5]) analyzing them under the Fourth Amendment. In *McLamb*, the Fourth Circuit rejected suppression in a similar circumstance. The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

McLamb, 880 F.3d at 691. Here, Investigator Matney followed the approach endorsed by *McLamb* by consulting with the U.S. Attorney's Office about geofence warrants. He then sought and obtained a search warrant from a U.S. Magistrate Judge. Investigator Matney thus did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. When police act in "objectively reasonable

5 The undersigned can only find six reported decisions pertaining to geofence warrants, all of which are cited within this memorandum brief. The earliest of those decisions was from July 2020, 20 months after the application for a geofence warrant in this matter.

reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate judge, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role…"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004*) (*quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case.

One case relevant to the discussion in this matter is *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022). The court in *Chatrie* provided a detailed account of the mechanisms behind a geofence search warrant. The District Judge in *Chatrie*, who was very clearly personally opposed to geofence warrants, found that the warrant at issue lacked particularized probable cause. However, the court grudgingly acknowledged that the good faith exception to the exclusionary rule applied and thus denied the defendant's motion to suppress. *Chatrie*, 590 F. Supp. 3d at 936-941. For similar reasons as those found by the court in *Chatrie*, at the very minimum, the good faith exception would likewise apply in the present matter.

The defendant argues that the good faith exception does not apply here because (1) the warrant was based on recklessly false statements; (2) the affidavit lacked a substantial basis to determine probable cause; and (3) the warrant was facially deficient. It should be noted that the threshold for establishing an exception to the good faith rule is a high one because officers

executing warrants cannot be expected to question the magistrate judge's probable-cause determination. *Messerschmidt*, 565 U.S. at 547. It is the magistrate judge's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting with the requirements of the Fourth Amendment. *Id*. The agent's belief that the warrant to Google was issued based on probable cause was not unreasonable and the good faith exception thus precludes suppression.

To specifically address the defendants' contentions, the second and third assertions have been discussed above in the section on probable cause (see pages 7 – 13). As to the allegation that the affidavit contains a misrepresentation of fact, this assertion is simply incorrect. In paragraph 16 of the affidavit, Inspector Matney avers that:

> Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs.

In fact, a review of the video shows exactly that. From approximately the 6:50 minute mark, when the assailant gets out of the white SUV and comes into view, to approximately the 9:50 minute mark, the assailant is seen walking around behind the Post Office with his left arm and hand up to his ear, as if he is holding a phone to his ear. (See Exhibit "A") While the security camera is too far away to see the phone, you can clearly see the position of the assailant's arm and hand in the normal position that people hold their arm and hand while talking on the phone. There is no other logical explanation for the position of the assailant's arm and hand for that length of time and it is certainly reasonable to view the video and believe that the assailant is talking on a cell phone. Inspector Matney's belief was indeed correct. Phone records later confirmed that McThunel had a phone conversation with Smith that lasted nearly six minutes, beginning at 5:16

p.m., which would have been just about the time that Ayodele was dropping McThunel off behind the Post Office.

Following the attack on Sylvester Cobbs, the assailant is seen pacing behind the Post Office when he sets the registered mail sacks down and appears to briefly reach into his pocket and glance down, as if checking his phone for messages. (See Exhibit "A") Later, the assailant was seen squatting behind the Post Office, and he appeared that he may have been checking his phone. (See Exhibit "A") While not conclusive, these portions of the video are certainly sufficient to believe that the assailant was "possibly using a cellular device." Accordingly, the defendants' argument that the affidavit contains a misrepresentation of fact is without merit.

C. Assertions of the Defendants

In their Memorandum of Authorities, the defendants assert four grounds in support of their Motion to Suppress: (1) misrepresentation of facts in the probable cause statement; (2) failure of the government to undertake "further legal process;" (3) the warrant violated the Fourth Amendment for various reasons; and (4) the good faith exception does not apply.

The first and fourth contentions have already been addressed herein. As set forth above, the assertion that the probable cause statement in the affidavit contained a misrepresentation of fact is simply incorrect. The government intends to offer further proof to address this issue at the hearing on the Motion to Suppress. Likewise, the assertion that the good faith exception does not apply has also been addressed above.

D. The Assertion that the Government Failed to Undertake "Further Legal Process"

The defendants, referencing Part II of Attachment A to the affidavit in support of the search warrant, state that the government failed to undertake "further legal process" as set forth in

numbered paragraph 2 under Part II. It is apparent that the defendants believe that "further legal process" means that the government has to return to the magistrate judge seeking another search warrant for each phase of the three-step geofence warrant process. To the contrary, Part II sets out the entire three-step process that was authorized by the magistrate judge when he issued the warrant. Step One requires Google to search its files and provide a list of accounts that were found within the geographical box during the designated time frame. These accounts will be given a numerical identifier so that the account subscribers will remain anonymous. Numbered paragraph 2, which sets forth Step One of the process, does state that additional information regarding the identified devices will come through "further legal process," but that process is then defined in numbered paragraphs 3 and 4. Step Two of the three-step process is set forth in numbered paragraph 3, which explains that for those accounts identified as relevant, Google shall provide additional location history outside of the predefined area to determine path of travel, which can, in some circumstances, assist the government in further narrowing down the list of accounts for which it needs identifying subscriber information. This additional location history is limited to 60 minutes on either side of the first and last timestamps associated with the account in the initial dataset. Numbered paragraph 4 then sets forth the final step of the three-step process, wherein Google will provide subscriber information for those accounts that the government identifies as relevant.

The government followed the three-step process specifically laid out in the affidavit and approved by the magistrate judge. There is no merit to the argument that failure to seek an additional search warrant at each step of the process violated the defendants' Fourth Amendment rights.

E. The Assertion that the Warrant Lacked Probable Cause

The defendants assert that the warrant lacked probable cause, arguing that cell phones and the data contained in them are granted heightened protections by the Fourth Amendment, the warrant lacked probable cause and was overbroad, and the warrant lacked particularity. Each of these arguments is without merit.

F. The Defendants Had No Reasonable Expectation of Privacy in Two[6] Hours of Google Location Information

As set forth below, the defendants had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the geofence warrant. The defendants argue that they had a reasonable expectation of privacy in their location information under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter*, 138 S. Ct. at 2217 n.3. Here, the government's acquisition of two hours of the defendants' location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government.[7]

6 Step One of the warrant limited the data requested to a one-hour time frame. Step Two of the warrant allowed the government to seek expanded data on relevant devices to sixty minutes either side of the first and last timestamp in the initial dataset for each device determined to be relevant to the investigation. For one relevant device the first and last timestamps were eight minutes apart. For the other relevant device the first and last timestamps were three minutes apart. Thus, the total time period for which data was obtained for each of the two relevant devices was just slightly more than two hours.

7 Google also disclosed to the government the defendants' basic subscriber information, including email address, Google Account ID, and Google services used. In *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010), the Fourth Circuit held that a subscriber has no reasonable expectation of privacy in such information.

1. Obtaining Two Hours of the Defendant's Location Information Was Not a Search Under *Carpenter*

The defendants claim, based on *Carpenter,* that they had a reasonable expectation of privacy in the two hours of location information disclosed by Google, but *Carpenter* does not bear the weight they place on it. In *Carpenter*, the Supreme Court determined that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 S. Ct. at 2217 and n.3.

The Supreme Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It explicitly declined to determine whether there is a "limited period" for which the government can acquire cell phone location information without implicating the Fourth Amendment. *Id.* at 2217 n.3. It also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because tower dump information is similar to the information disclosed pursuant to the Geofence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the Geofence warrant sought information on all devices that were within a particular area during a particular interval.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it is not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a

comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216-17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220.

By this standard, the government did not conduct a search when it obtained the defendants' location information pursuant to the geofence warrant. Two hours of location data is only 1/84th of the period that *Carpenter* held constituted a search, and it does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. Rather than providing an encyclopedic chronicle of the defendants' lives, the information disclosed by Google provided a summary of their location for a brief period of time late in the afternoon of February 5, immediately before, during, and after the robbery and assault of a postal employee. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

The Seventh Circuit has held that *Carpenter* "does not help" a robber identified via tower dumps. *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The court explained that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near one location (the victim stores) at one time (during the robberies))." *Id.* at 611.

2. The Defendants Have No Reasonable Expectation of Privacy in Location Information They Disclosed to Google

Because *Carpenter* does not create a reasonable expectation of privacy in two hours of location information, Google's disclosure of that information to the government is subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the government. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to the defendants' location information.

For example, in *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. First, the Court stated that "we doubt that people in general entertain any

actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. In addition, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted). The Court explained that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44.

The defendants therefore had no reasonable expectation of privacy in Google's records of their location because they voluntarily conveyed their location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, the defendants had previously taken an affirmative step to disclose their location information to Google. Moreover, they agreed that Google would have access to their location information for purposes ranging from providing them with targeted advertising or assistance with driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). These facts demonstrate that the defendants voluntarily disclosed their location information to Google and the government did not infringe their reasonable expectation of privacy when it obtained from Google information about their device's location during a two-hour interval.

The principle that the government may obtain information revealed to a third party has deep roots. The Supreme Court has recognized that "as early as 1612, … Lord Bacon is reported to have declared 'all subjects, without distinction of degrees, owe to the King tribute and service,

not only of their deed and hand, but of their knowledge and discovery.'" *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). Similarly, the Court has recognized that it is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). In this case, Google was a witness to the robbery; it had information regarding the Postal Service robbery in a database which it accessed and used to provide services to its users and advertisers. The public had a right to Google's evidence, and the Fourth Amendment did not bar the United States from obtaining that evidence from Google.

Finally, the fact that the defendants voluntarily disclosed their location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected "without any affirmative act on the part of the user beyond powering up" and that "there is no way to avoid leaving behind a trail of location data." *Id.* In contrast, in order for Google to have his location information, the defendant had to affirmatively opt in, and he also retained the ability to delete his information. Finally, a cell phone user's disclosure of location information to

the phone company is merely incidental to receiving communication service from the company, but a device owner's disclosure of location information to Google is the central prerequisite to obtaining Google location services. The defendants thus voluntarily disclosed their location information to Google, and Google's disclosure of that information to the government did not infringe upon their reasonable expectation of privacy.

G. Additional Cases Pertaining to Geofence Warrants

The government has found six cases that address the issue of geofence warrants. In addition to *Google V* and *Chatrie*, referenced above, the other cases can be found at 2020 WL 5491763 (E.D. Ill. 2020) (*Google I*), 481 F. Supp. 3d 730 (E.D. Ill. 2020) (*Google II*), 497 F. Supp. 3d 345 (E.D. Ill. 2020) (*Google III*), and 542 F. Supp. 3d 1153 (D. Kan. 2021) (*Google IV*). Interestingly, three of those cases arise from the Eastern District of Illinois and two of those, *Google I* and *Google II*, involve the same investigation. Of the reported decisions, three are magistrate judge decisions that deny the requested search warrants from the outset (*Google I*, *Google II*, and *Google IV*), two are magistrate judge decisions that grant the request for the search warrant (*Google III* and *Google V*), and one is a District Court decision that denies a motion to suppress a geofence warrant that has already been issued (*Chatrie*). Although only a handful of written decisions are available, thousands of geofence warrants have been issued in the last few years, and while numbers are unknown, if *Google I*, *II*, and *IV* are any indication, likely some geofence applications have been denied. See *Google V*, 579 F. Supp. 3d at 67-68 and n. 3. Even the reported decisions that deny geofence applications admit that geofence warrants are not categorically unconstitutional. *Google II*, 481 F. Supp. 3d at 756, *see also Google I*, 2020 WL 5491763, at *7 (offering advice on how the warrant could be revised to pass constitutional

scrutiny); *Google IV*, 542 F. Supp. 3d at 1158-1159 (court specifically left open the possibility that the application could be revised to pass constitutional scrutiny).

Rather than attempt to distinguish the three reported magistrate judge decisions in which a geofence warrant was denied, the government would simply state that each case is unique and the court must decide in each case whether the government has made the requisite showing of probable cause and particularity. For the reasons set forth herein, the government has shown that in this particular matter, the geofence warrant has met all constitutional demands.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the defendants' Motion to Suppress be denied.

Respectfully submitted, this the 15th day of November, 2022.

CLAY JOYNER
United States Attorney

By: *s/ Robert J. Mims*
ROBERT J. MIMS
Assistant United States Attorney
Ethridge Professional Building
900 Jefferson Avenue
Oxford MS 38655-3608
Telephone 662/234-3351
Criminal Division fax 662/234-0657

CERTIFICATE OF SERVICE

I hereby certify that on November 15, 2022, I electronically filed the foregoing with the Clerk of the Court using the ECF system which sent notification of such filing to the following:

Goodloe Lewis, Esq.
glewis@hickmanlaw.com

Paul Chiniche, Esq.
pc@chinichelawfirm.com

Bill Travis, Esq.
bill@southavenlaw.com

s/ Robert J. Mims
ROBERT J. MIMS
Assistant United States Attorney